CLAIM SET AS AMENDED

1. (Currently Amended) A conditional access system comprising:

a demultiplexer for demultiplexing a packet stream transmitted from a transmitting site into encrypted coded media data, an ECM (Entitlement Control Message) and an EMM (Entitlement Management Message);

an EMM decryption section for retrieving work keys and ~~subscriber contract~~ partial viewing authorization information from the EMM extracted by said demultiplexer;

~~means for retrieving partial viewing authorization information included in one of the EMM and ECM extracted by said multiplexer;~~

an ECM decryption section for decrypting the ECM using the work keys[[,]] and for intermittently retrieving scrambling keys from the ECM, when the partial viewing authorization information retrieved by said EMM decryption section permits partial viewing; ~~and~~

~~outputting means for descrambling and decoding part of the coded media data using the scrambling keys when the partial viewing authorization information permits partial viewing, and for outputting the partially decoded coded media data~~

a media descrambling section for intermittently descrambling the coded media data using the scrambling keys intermittently retrieved by said ECM decryption section; and

a decoding section for decoding the coded media data intermittently descrambled by said media data descrambling section.

2. (Currently Amended) The conditional access system according to claim 1, wherein said ECM decryption section ~~comprises:~~

~~means for intermittently retrieving the scrambling keys from the ECM when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing, and wherein said outputting means comprises:~~

~~a media data descrambling section for descrambling the coded media data using the scrambling keys retrieved by said ECM decryption section; and~~

~~a decoding section for decoding the coded media data descrambled by said media data descrambling section~~ retrieves only part of the scrambling keys included in the ECM.

3. (Currently Amended) The conditional access system according to claim [[2]] 1, wherein said ~~means for intermittently retrieving the scrambling keys comprises:~~

~~a decryption validity decision section for outputting decryption control information in response to the subscriber contract information and the partial viewing authorization information; and~~

~~a decryption processor for intermittently retrieving the~~

~~scrambling keys from the ECM in response to the decryption control information when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing~~ ECM decryption section retrieves all the scrambling keys included in the ECM and supplies said media data descrambling section with only part of the scrambling keys.

4. (Currently Amended) ~~The conditional access system according to claim 2, wherein said means for intermittently retrieving the scrambling keys comprises:~~

~~a decryption processor for retrieving all scrambling keys included in the ECM;~~

~~a scrambling key output validity decision section for outputting output control information in response to the subscriber contract information and the partial viewing authorization information; and~~

~~an output controller for supplying said media data descrambling section with only part of the scrambling keys in response to the output control information when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing~~

A conditional access system comprising:

a demultiplexer for demultiplexing a packet stream transmitted from a transmitting site into encrypted coded media data, an ECM

(Entitlement Control Message) and an EMM (Entitlement Management Message);

an EMM decryption section for retrieving work keys and partial viewing authorization information from the EMM extracted by said demultiplexer;

an ECM decryption section for decrypting the ECM using the work keys retrieved by said EMM decryption section and for retrieving scrambling keys from the ECM;

a media descrambling section for intermittently descrambling the coded media data using the scrambling keys when the partial viewing authorization retrieved by said EMM decryption section permits partial viewing; and

a decoding section for decoding the coded media data intermittently descrambled by said media data descrambling section.

5. (Currently Amended) The conditional access system according to claim [[1]] 4, wherein said ~~outputting means comprises:~~

~~a media data descrambling section for intermittently descrambling the coded media data using the scrambling keys when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing; and~~

~~a decoding section for decoding the coded media data descrambled by said media data descrambling section~~ media data

descrambling section handles part of the coded media data which is not descrambled as unencrypted data.

6. (Currently Amended) ~~The conditional access system according to claim 5, wherein said media data descrambling section comprises:~~

~~a descramble validity decision section for outputting descramble control information alternately authorizing and inhibiting descrambling when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing;~~

~~a descrambler for descrambling part of the coded media data in response to the descramble control information; and~~

~~a scramble control information modifier for handling part of the coded media data which is not descrambled as unencrypted data~~ A conditional access system comprising:

a demultiplexer for demultiplexing a packet stream transmitted from a transmitting site into encrypted coded media data, an ECM (Entitlement Control Message) and an EMM (Entitlement Management Message);

an EMM decryption section for retrieving work keys and partial viewing authorization information from the EMM extracted by said demultiplexer;

an ECM decryption section for decrypting the ECM using the work keys retrieved by said EMM decryption section and for

retrieving scrambling keys from the ECM;

a media descrambling section for descrambling the coded media data using the scrambling keys retrieved by said ECM decryption section; and

a decoding section for intermittently decoding the coded media data descrambled by said media data descrambling section when the partial viewing authorization information retrieved by said EMM decryption section permits partial viewing.

7. (Currently Amended) The conditional access system according to claim [[1]] 6, wherein said ~~outputting means comprises:~~

~~a media data descrambling section for descrambling the coded media data using the scrambling keys retrieved by said ECM decryption section; and~~

~~a~~ decoding section ~~for intermittently decoding the coded media data descrambled by said media data descrambling section, when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing~~ decodes only part of frames in a frame sequence constituting the coded media data.

8. (Currently Amended) The conditional access system according to claim 7, wherein said decoding section ~~comprises:~~

~~a decoding validity decision section for outputting decoding~~

~~control information in response the subscriber contract information and the partial viewing authorization information; and~~

~~a decoding processor for decoding only part of frames in a frame sequence constituting the coded media data in response to the decoding control information when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing~~ decodes only I frames.

9. (Currently Amended) The conditional access system according to claim [[8]] 6, wherein said decoding ~~processor~~ section decodes ~~only I frames in response to the decoding control information when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing~~ all the coded media data descrambled by said media data descrambling section and supplies only part of the decoded coded media data to a television receiver.

10. (Currently Amended) ~~The conditional access system according to claim 7, wherein said decoding section comprises:~~

~~a decoding processor for decoding all the coded media data descrambled by said media data descrambling section; and~~

~~a media display controller for supplying only part of the descrambled coded media data to a television receiver when the subscriber contract information inhibits viewing and the partial~~

~~viewing authorization information permits partial viewing~~

A conditional access system comprising:

a demultiplexer for demultiplexing a packet stream transmitted from a transmitting site into encrypted coded media data, an ECM (Entitlement Control Message) and an EMM (Entitlement Management Message);

an EMM decryption section for retrieving partial viewing authorization information from the EMM extracted by said demultiplexer, said EMM decryption section intermittently retrieving work keys from the EMM when the partial viewing authorization information permits partial viewing;

an ECM decryption section for intermittently decrypting the ECM using the work keys intermittently retrieved by said EMM decryption section and for intermittently retrieving scrambling keys from the ECM;

a media descrambling section for intermittently descrambling the coded media data using the scrambling keys intermittently retrieved by said ECM decryption section; and

a decoding section for decoding the coded media data intermittently descrambled by said media data descrambling section.

11. (Currently Amended) The conditional access system according to claim 10, wherein said ~~outputting means comprises:~~

~~a media data descrambling section for descrambling the coded~~

~~media data using the scrambling keys retrieved by said ECM decryption section; and~~

~~a decoding section for decoding the coded media data descrambled by said media data descrambling section, for storing the decoded coded media data into a memory on a block by block basis, and for outputting the blocks with changing their sequence when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing~~ EMM decryption section retrieves only part of the work keys included in the EMM.

12. (Currently Amended) The conditional access system according to claim 10, wherein said EMM decryption section ~~comprises means for intermittently retrieving work keys from the EMM when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing, wherein said ECM decryption section decrypts the ECM using the work keys and retrieves scrambling keys from the ECM, and wherein said outputting means comprises:~~

~~a media data descrambling section for descrambling the coded media data using the scrambling keys retrieved by said ECM decryption section; and~~

~~a decoding section for decoding the coded media data descrambled by said media data descrambling section~~ retrieves all

the work keys included in the EMM and supplies only part of the work keys to said ECM decryption section.

13. (Currently Amended) The conditional access system according to claim 1 [[12]], wherein said ~~means for intermittently retrieving work keys comprises:~~

~~a decryption validity decision section for outputting decryption control information in response to the subscriber contract information and the partial viewing authorization information; and~~

~~a decryption processor for retrieving only part of the work keys from the EMM in response to the decryption control information when the subscriber contract information inhibits viewing and the partial viewing authorization information permits partial viewing~~ ECM decryption section, instead of said EMM decryption section, retrieves the partial viewing authorization information from the ECM when the partial viewing authorization information is included in the ECM.

14. (Currently Amended) The conditional access system according to claim 1 [[12]], wherein ~~said means for intermittently retrieving work keys comprises:~~

~~a decryption processor for retrieving all the work keys included in the EMM;~~

~~a work key output validity decision section for outputting output control information about the work keys in response to the subscriber contract information and the partial viewing authorization information; and~~

~~a work key output controller for supplying only part of the work keys to said ECM decryption section in response to the output control information when the subscriber contract information inhibits viewing and~~ the partial viewing authorization information ~~permits partial viewing~~ includes a control parameter indicating a partially authorized viewable range.

15. (Currently Amended) The conditional access system according to claim 1, wherein the partial viewing authorization information ~~includes a control parameter indicating a partially authorized viewable range~~ consists of information authorizing viewing only for a specific time period.

16. (Currently Amended) The conditional access system according to claim 1, wherein ~~the partial viewing authorization information consists of information authorizing viewing only for a specific time period~~ a subscriber contract information that includes information authorizing partial viewing is used as the partial viewing authorization information.

17. (Currently Amended) The conditional access system according to claim 1, wherein the ~~subscriber contract information that includes information authorizing partial viewing is used as the partial viewing authorization information~~ EMM is used for inserting the work keys which are used only for specific time periods.

18. (Currently Amended) The conditional access system according to claim 1, wherein ~~the EMM is used into which the work keys are inserted only for specific time periods~~ said demultiplexer and said decoding section are based on the MPEG-2 standard.

19. (Currently Amended) The conditional access system according to claim 1, wherein ~~said demultiplexer and said decoding section are based on the MPEG-2 standard~~ when a plurality of programs are multiplexed into the packet stream transmitted from the transmitting site, authorization, partial authorization and inhibition of viewing the programs are determined for individual programs independently.

20. (Canceled).